# Introduction to Safety Systems in Research Accelerators

Safety System Management

USPAS

June, 2004

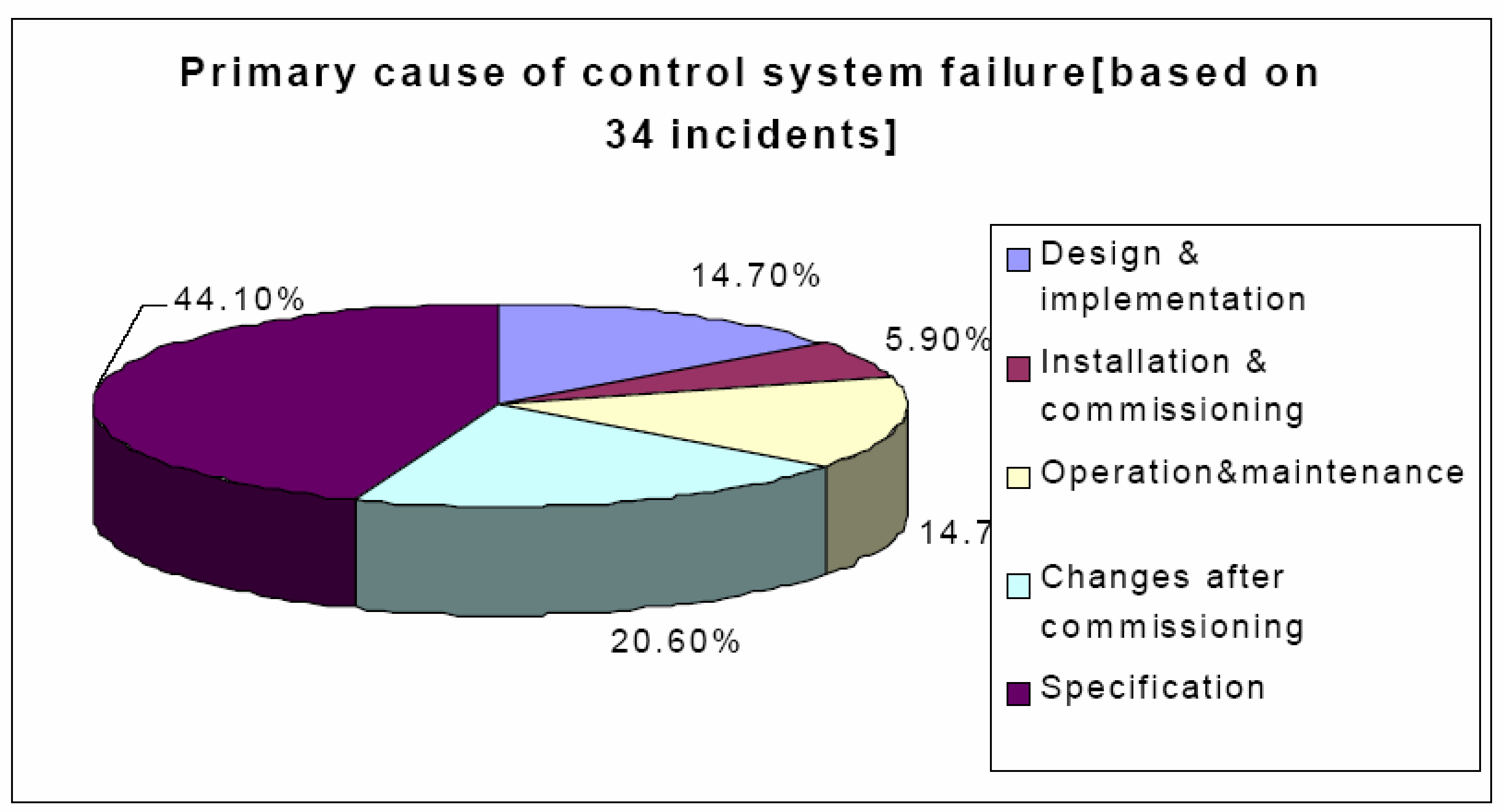
# Elements of SS Management

- The objective of safety system management is to ensure that the desired level of risk reduction is maintained over the lifetime of the system.
- In reality, and in accordance with the ALARP principle, there is a continual vigilance of and incremental improvement in the integrity of the system and how it is used.
- This involves all persons that are affected by the operation and use of the system.

# Management of Change

- Ensure that lifecycle is not broken
- Established procedures for change
- Plan for decommissioning

# HSE Report on Causes of Safety System Failure



Primary cause of control system failure[based on 34 incidents]

# IEC61508 – SS Management Requirements

Those organizations or individuals that have overall responsibility for one or more phases of the overall [*safety system*] in respect of those phases for which they have overall responsibility, specify all management and technical activities that are necessary to ensure that the safety-related systems achieve and maintain the required functional safety. In particular, the following should be considered:

a) the policy and strategy for achieving functional safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organization to ensure a culture of safe working;

b) identification of the persons, departments and organizations which are responsible for carrying out and reviewing the applicable overall [*safety system*] lifecycle phases (including, where relevant, licensing authorities or safety regulatory bodies);

c) the overall [*safety system*] lifecycle phases to be applied;

d) the way in which information is to be structured and the extent of the information to be documented;

# IEC61508 – SS Management Requirements

e) the selected measures and techniques used to meet the requirements of a specified [*requirement*]

f) the functional safety assessment activities

g) the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations relating to E/E/PE safety-related systems arising from

- – hazard and risk analysis
- – functional safety assessment
- – verification activities
- – validation activities
- – configuration management

h) the procedures for ensuring that applicable parties involved in any of the overall [*safety system*] lifecycle activities are competent to carry out the activities for which they are accountable; in particular, the following should be specified:

- – the training of staff in diagnosing and repairing faults and in system testing;
- – the training of operations staff;
- – the retraining of staff at periodic intervals;

i) the procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations made to minimise the probability of a repeat occurrence;

# IEC61508 – SS Management Requirements

j) the procedures for analysing operations and maintenance performance. In particular procedures for – recognising systematic faults which could jeopardise functional safety, including procedures used during routine maintenance which detect recurring faults;

- – assessing whether the demand rates and failure rates during operation and maintenance are in accordance with assumptions made during the design of the system;

k) requirements for periodic functional safety audits in accordance with this subclause including

- – the frequency of the functional safety audits;
- – consideration as to the level of independence required for those responsible for the audits;
- – the documentation and follow-up activities;

l) the procedures for initiating modifications to the safety-related systems;

m) the required approval procedure and authority for modifications;

# IEC61508 – SS Management Requirements

n) the procedures for maintaining accurate information on potential hazards and safety-related systems;

o) the procedures for configuration management of the [*safety system*] during the overall [*safety system*] lifecycle phases; in particular the following should be specified:

- – the stage at which formal configuration control is to be implemented;
- – the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
- – the procedures for preventing unauthorized items from entering service;

p) where appropriate, the provision of training and information for the emergency services.

# Management of Management

Management must understand their responsibilities

- Assume responsibility for acceptable level of risk
- Provide staff adequate resources and training
- Establishment of policy and strategy for achieving safety goals

# Step 1:  Policy

- Senior management provides
  - Establish expectations
  - Sources of info
    - Institutional plans
    - Strategic plans
    - Contract requirements
    - External/internal commitments

# Step 2: Planning

- Defining work scope
- Budget
- Timelines
- Hazard identification & characterization
- System Interfaces

# Step 2:  Planning

- Civil construction or modifications
  - Access Control
  - Life Safety
  - Shielding
  - Potential impact on SS hardware
- Potentially hazardous equipment design, development, and modification.
  - Shutdown Methods
  - Status Feedback

# Step 2: Planning

- Spare parts
- Determine the level of review and approval needed to bring system into operation
  - Readiness Review
  - Peer Review (internal or external; formal or informal)
- Start configuration management (CM) program development early

# Purpose of CM Program

- The purpose of the Configuration Management (CM) Program is to establish the CM mechanisms for consistency between the appropriate design requirements, physical configuration, and documentation of critical items necessary to protect workers and the public during the lifecycle of a facility.

# Configuration Management (CM)

- Consists of 5 components
  - Program Management
  - Design Requirements
  - Document Control
  - Change Control
  - Assessments
- Graded Approach

# CM: Program Management

- Identify critical items based on facility safety basis documents
- Determine the configuration level for each critical item
- Establish a system for controlling changes
  - How, and by whom, shall changes be reviewed
  - Who has approval authority for changes

# CM:  Design Requirements

- Documents are added, changed, or deleted using the change control process which ensures the current configurations are known and controlled at all times.
- Interfaces with other systems are clearly identified.
- Identifying interfaces is important both for clearly identifying the scope of the CI and for interfacing systems that may have different CM levels or CM owners.

# CM: Document Control

- Identify the types and specific documents to be included within the CM Program.
- Determine how they will be stored to protect them from loss or damage.
- How will the documents & drawing be numbered and tracked so that you are sure most current documents are in use?
- Ensure documents can be easily retrieved

# Step 3: Implementation & Operation

- Develop Users' Manual and other work procedures documents
  - Sweep procedures
  - Certification procedures/checklists
  - Integrate into facility operational procedures
  - Maintenance procedures
  - Safety system bypass CM requirements
  - Troubleshooting guides
  - Training/education documents
  - Change Control procedures

# CM: Change Control

- The objective of the change control element is to maintain consistency among the design requirements, physical configuration, and facility documentation as changes are made.
- This objective can be met if needed changes to a CI are properly identified, evaluated for impact to safety and to other components of the CI, executed in a controlled manner, and verified when complete.

# Change Control

- Changes may include changes to hardware, maintenance procedures, processes, operations, documents, computer software, and inventory limits, as well as temporary modifications.
- Review each specific proposed change to determine whether it is within the bounds of the design requirements
- Ensure affected parties are made aware of the change.

# System Maintenance

- Don’t rely on “reactive maintenance”
- Instead, focus on
    - Preventive maintenance
    - Training
    - Spare part quality
    - Design improvements

# Step 4: Checking & Corrective Action

- Assessments also 5th element of CM program
- Should be conducted periodically during the life of the system
- Should also be conducted whenever a change or modification is performed that impacts the safety basis

# Step 4: Checking & Corrective Action

- Documented
- Corrective actions tracked
- Evaluated for trends and opportunities for continuous improvement

# Step 5:  Management Review

- Top management should periodically review system management to ensure it is meeting performance expectations
  - Line Self-Assessments
  - Contract performance review

# Why Quality Initiatives Fail

- Quality programs often struggle to gain initial acceptance and to sustain continuous improvement. (U.S. General Accounting Office, 1991)

- The inability to manage an improvement program as a dynamic process is the main determinant of program failure.

# Certification

- Safety systems require periodic certification in order to uncover dangerous undetected failures.
- Exercises all components of a system
- Should have an independent reviewer

# Training

- SS Designers
- Maintenance Personnel
- Machine Operators
- Management

# Bypass

- Bypassing of safety system components during the lifetime of a facility is inevitable.
  - Final devices should have a manual energy isolation method that will provide equivalent protection as the automated safety system, e.g. lock out/tag out.  This should be in the design requirements for the device.